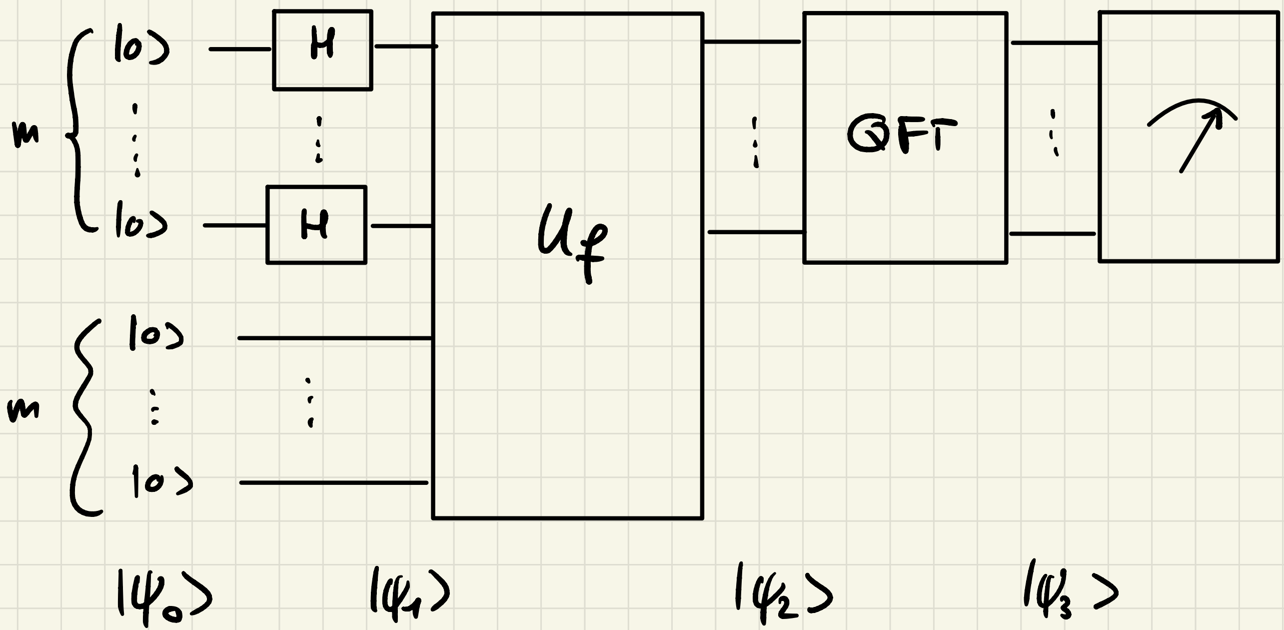
Quantum computation: lecture 8

As a reminder, we were considering the following circuit for Shor's algorithm:



Remember also that we are looking for the period r of $f: \{0..M-1\} \longrightarrow \{0..M-1\}$ defined as $f(x) = a^x \bmod N$

For now, we assume that $M = 2^m$ for some $m \geq 1$ and also that $M = k \cdot r$ for some $k \geq 1$ (note that these two assumptions contradict themselves but the plan is to remove the second one later)

So far, we have computed

$$|\psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{\frac{M}{r}-1} |x_0 + jr\rangle \otimes |\underbrace{f(x_0+jr)}_{=f(x_0)}\rangle$$

and recall that

$$QFT\,|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \exp\left(\frac{2\pi i x y}{M}\right) |y\rangle$$

From there, let us proceed to compute

$$|\psi_3\rangle = \left(QFT \otimes I^{\otimes m}\right) |\psi_2\rangle$$

$$|\psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{\frac{M}{r}-1} QFT\,|x_0+jr\rangle \otimes |f(x_0)\rangle$$

$$= \frac{1}{M} \sum_{x_0=0}^{r-1} \sum_{j=0}^{\frac{M}{r}-1} \sum_{y=0}^{M-1} \exp\left(\frac{2\pi i (x_0+jr)y}{M}\right) |y\rangle \otimes |f(x_0)\rangle$$

note that an extra factor $1/\sqrt{M}$ appears here

$$= \frac{1}{M} \sum_{x_0=0}^{r-1} \sum_{y=0}^{M-1} e^{\frac{2\pi i x_0 y}{M}} \underbrace{\left(\sum_{j=0}^{\frac{M}{r}-1} e^{\frac{2\pi i j r y}{M}} \right)}_{} |y\rangle \otimes |f(x_0)\rangle$$

$$= \begin{cases} M/r & \text{if } y \text{ is a multiple of } \frac{M}{r} \\ 0 & \text{otherwise} \end{cases}$$

So the sum over $y \in \{0..M-1\}$ can be rewritten as a sum over $k \in \{0.. r-1\}$ with $y = k \cdot \frac{M}{r}$:

$$|\varphi_3\rangle = \frac{1}{\cancel{M}} \cdot \frac{\cancel{M}}{r} \sum_{x_0=0}^{r-1} \sum_{k=0}^{r-1} e^{\frac{2\pi i x_0 k}{r}} \left| k \cdot \frac{M}{r} \right\rangle \otimes |f(x_0)\rangle$$

<u>Measurement</u> : Measuring the first m qubits in the computational basis, the output state is

$$|\varphi_4\rangle = \frac{P_{y_0} |\varphi_3\rangle}{\| P_{y_0} |\varphi_3\rangle \|} \quad \text{where } P_{y_0} = |y_0\rangle\langle y_0| \otimes I_m$$

with probability

$$P(y_0) = \langle \psi_3 | P_{y_0} | \psi_3 \rangle$$

$$= \left(\frac{1}{r} \sum_{x_0,k=0}^{r-1} e^{-2\pi i x_0 k/r} \langle k\tfrac{\Pi}{r}| \otimes \langle f(x_0)| \right) \cdot \left(|y_0\rangle\langle y_0| \otimes I_m \right)$$

$$\cdot \left(\frac{1}{r} \sum_{x_0',k_0'=0}^{r-1} e^{2\pi i x_0' k'/r} |k'\tfrac{\Pi}{r}\rangle \otimes |f(x_0')\rangle \right)$$

$$= \frac{1}{r^2} \sum_{x_0,k,x_0',k'=0}^{r-1} e^{2\pi i (x_0'k' - x_0 k)/r} \underbrace{\langle k\tfrac{\Pi}{r}|y_0\rangle \cdot \langle y_0 | k'\tfrac{\Pi}{r}\rangle}_{= \delta_{k\frac{\Pi}{r},y_0} \cdot \delta_{k'\frac{\Pi}{r},y_0}} \cdot \underbrace{\langle f(x_0)|f(x_0')\rangle}_{= \delta_{x_0 x_0'}}$$

remember that f differs across $0 \leq x_0 \leq r-1$

So finally

$$P(y_0) = \begin{cases} \frac{1}{r^2} \sum_{x_0=0}^{r-1} 1 = \frac{1}{r} & \text{if } y_0 \text{ is a multiple of } \frac{M}{r} \\ 0 & \text{otherwise} \end{cases}$$

i.e. the circuit outputs $y_0 = k \cdot \frac{M}{r}$ $\quad 0 \leq k \leq r-1$ with uniform probability. Let us see what we can deduce from this...

- If $\gcd(k,r)=1$, then simplifying the fraction $\frac{y_0}{M}=\frac{k}{r}$, we obtain the value of r by looking at the final denominator.
- If $\gcd(k,r)\neq 1$, this procedure fails.

In practice, we do not know whether $\gcd(k,r)=1$ or not, but we can still simplify the fraction and test whether the resulting denominator is a period of f.

As $0 \leq k \leq r-1$ is uniform, the success probability of this procedure is therefore given by

$$\mathbb{P}\left(\gcd(k,r)=1\right) = \frac{\varphi(r)}{r}$$

where $\varphi(r) = \#\{0 \leq k \leq r-1 : \gcd(k,r)=1\}$

the Euler function

It can be shown that $\varphi(r) \geq \dfrac{r}{4\ln(\ln r)}$,

so $$\mathbb{P}(\text{success}) \geq \frac{1}{4\ln(\ln r)}$$

As $r \leq M$, this further implies (for one measurement):

$$\mathbb{P}(\text{success}) \geq \frac{1}{4 \ln(\ln M)}$$

Therefore, $\mathbb{P}(\text{failure}) \leq \varepsilon$ after T trials if $T \geq 4 \ln(\ln M) \cdot |\ln \varepsilon|$ (same reasoning as for Simon's algorithm).

And now for the real thing...

First of all, let us see what happens when we remove the unnatural assumption that M is a multiple of r (but it still holds that $M = 2^m$ for some $m \geq 1$).

In this case, define for $0 \leq x_0 \leq r-1$:

$$A(x_0) = \inf\{ j \geq 1 : x_0 + jr > M-1 \}$$

(Note that when M is a multiple of r, then $A(x_0) = \frac{M}{r} \quad \forall\, 0 \leq x_0 \leq r-1$)

- So in this general case, state $|\varphi_2\rangle$ is given by

$$|\varphi_2\rangle = \frac{1}{\sqrt{M}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{A(x_0)-1} |x_0 + jr\rangle \otimes |f(x_0)\rangle$$

- Likewise, $|\varphi_3\rangle$ is given by

$$|\varphi_3\rangle = \frac{1}{M} \sum_{x_0=0}^{r-1} \sum_{y=0}^{M-1} e^{\frac{2\pi i x_0 y}{M}} \underbrace{\left(\sum_{j=0}^{A(x_0)-1} e^{\frac{2\pi i j r y}{M}} \right)}_{\text{but this term now is not anymore either } \frac{M}{r} \text{ or } 0 \ldots} |y\rangle \otimes |f(x_0)\rangle$$

- After the measurement, the output state is $|y_0\rangle$ with probability

$$P(y_0) = \langle \psi_3 | \left(|y_0\rangle\langle y_0| \otimes I_m \right) | \psi_3 \rangle$$

$$= \frac{1}{M} \sum_{x_0=0}^{r-1} \sum_{y=0}^{M-1} e^{\frac{-2\pi i x_0 y}{M}} \left(\sum_{j=0}^{A(x_0)-1} e^{\frac{-2\pi i j y}{M/r}} \right)$$

$$\cdot \frac{1}{M} \sum_{x_0'=0}^{r-1} \sum_{y'=0}^{M-1} e^{\frac{+2\pi i x_0' y'}{M}} \left(\sum_{j'=0}^{A(x_0')-1} e^{\frac{2\pi i j' y'}{M/r}} \right)$$

$$\cdot \langle y | y_0 \rangle \cdot \langle y_0 | y' \rangle \cdot \langle f(x_0) | f(x_0') \rangle \quad \left(\begin{array}{l} = \delta_{y y_0} \\ \cdot \delta_{y' y_0} \\ \cdot \delta_{x_0 x_0'} \end{array} \right)$$

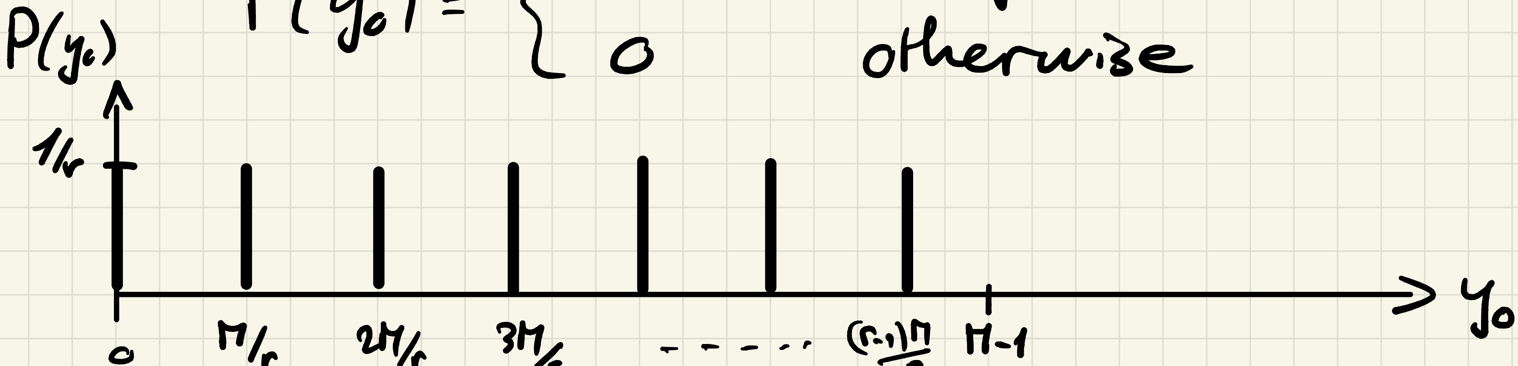
which gives after simplification

$$P(y_0) = \frac{1}{M^2} \cdot \sum_{x_0=0}^{r-1} \left| \sum_{j=0}^{A(x_0)-1} e^{\frac{2\pi i j y_0}{M/r}} \right|^2$$

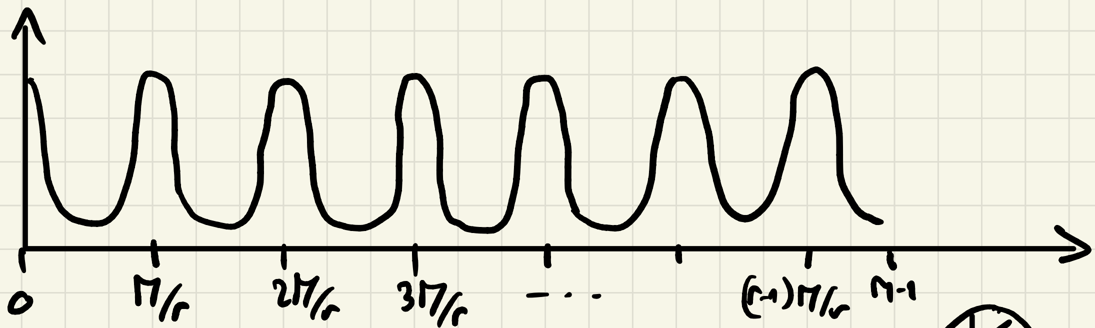
As seen above:

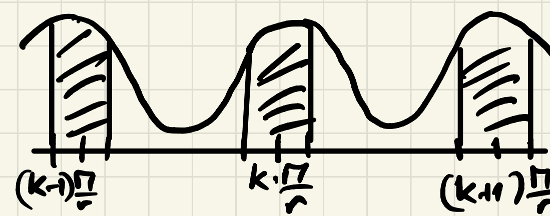
when $M = k \cdot r$, this expression simplifies to

$$P(y_0) = \begin{cases} 1/r & \text{if } y_0 = \text{multiple of } r \\ 0 & \text{otherwise} \end{cases}$$



In the general case, the picture is as follows:





Lemma (without proof)

Let $I = \bigcup_{k=0}^{r-1} I_k$ with $I_k = \left[k \cdot \frac{M}{r} - \frac{1}{2}, k \cdot \frac{M}{r} + \frac{1}{2}\right]$

(note $|I_k| = 1 \ \forall k$)

Then $\mathbb{P}(y_0 \in I) \geq \frac{2}{5}$

Last steps left for next week:

- Conclusion of the algorithm (how to find r from the observation of y_0)
- Construction of the QFT circuit
- Construction of the oracle U_f circuit for $f(x) = a^x \pmod N$

<u>Side note</u>: simple and elegant proof that the Euler totient function satisfies $\varphi(n) \geq \frac{n}{4\ln(n)}$

Let $n = p_1^{a_1} \cdots p_k^{a_k}$ be the decomposition of n

Then $\varphi(n) = \#\{1 \leq a \leq n : \gcd(a,n) = 1\}$

$$= p_1^{a_1-1}(p_1-1) \cdot \ldots \cdot p_k^{a_k-1}(p_k-1)$$

<u>Ex</u>: If $n = p \cdot q$, then $\varphi(n) = (p-1)\cdot(q-1)$

If $n = p^k$, then $\varphi(n) = p^{k-1}(p-1)$

$$\text{So} \quad \frac{\varphi(m)}{m} = \frac{p_1^{a_1-1}(p_1-1) \cdots p_k^{a_k-1}(p_k-1)}{p_1^{a_1} \cdots p_k^{a_k}}$$

$$= \prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right) = \prod_{j=1}^{k}\left(1-\frac{1}{p_j^2}\right) \Big/ \prod_{j=1}^{k}\left(1+\frac{1}{p_j}\right)$$

$$\geq \frac{\prod_{i=2}^{m}\left(1-\frac{1}{i^2}\right)}{\prod_{j=1}^{k}\left(1+\frac{1}{p_j}\right)} \geq \frac{\prod_{i=2}^{m}\frac{(i-1)(i+1)}{i^2}}{1+\sum_{i=2}^{m}\frac{1}{i}} \leftarrow \left(\begin{array}{l}\text{expand the}\\ \text{product}\end{array}\right)$$

$$\geq \frac{\frac{1\cdot\cancel{3}}{2^2}\cdot\frac{2\cdot\cancel{4}}{\cancel{3}^2}\cdot\frac{\cancel{3}\cdot\cancel{5}}{\cancel{4}^2}\cdot\frac{\cancel{4}\cdot 6}{\cancel{5}^2}\cdot\frac{\cancel{5}\cdot 7}{6^2}\cdots}{1+\ln(m)} \geq \frac{1}{4\ln(m)}$$

#